KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN: 249203)
ak@kazlg.com
David J. McGlothlin, Esq. (SBN: 253265)
david@kazlg.com
Mona Amini, Esq. (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff,
Brett Garrote

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

BRETT GARROTE, individually an on behalf of all others similarly situated,

Plaintiff,

vs.

TRISTAR INSURANCE GROUP, INC.

Defendant(s).

Case No.:

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*;
3. CALIFORNIA CUSTOMER RECORDS ACT. CAL. CIV. CODE §§ 1798.80, *et seq.*;
4. NEGLIGENCE;
5. NEGLIGENCE *PER SE;*
6. INVASION OF PRIVACY;
7. BREACH OF IMPLIED CONTRACT; and
8. BREACH OF CONTRACT

JURY TRIAL DEMANDED

//

//

//

//

INTRODUCTION

Plaintiff BRETT GARROTE (hereinafter "Plaintiff"), individually and on behalf of all others similarly situated (the "Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to himself and on information and belief as to all other matters, bring this class action 28 U.S.C. § 1332(d) against TRISTAR INSURANCE GROUP, INC. (hereinafter "Defendant"), and allege as follows:

NATURE OF THE CASE

1. This is a data breach class action arising out of Defendant's and their related entities, subsidiaries, and agents' failure to implement and maintain reasonable security practices to protect consumers' sensitive personal information that Defendant collected and maintained from Plaintiff and the Class members. Defendant further failed to provide timely and adequate notice to Plaintiff and other Class members that their information had been stolen. Defendant is among the nation's leading resources for workers' compensation, property and casualty programs, and risk control[1] that manages more than 350 alternatively funded entities in both the private and public insurance segments.[2] For their business purposes, Defendant obtains, stores, and transmits a substantial amount of personally identifiable information ("PII") from individuals,[3] like Plaintiff, in their servers and/or networks, including but not limited to their name, date of birth, and Social Security Number.

2. On or about February 1, 2024, data breach notice letters were issued by or on behalf of Defendant announcing that on or about November 10, 2022, Defendant became aware of suspicious activity on certain computer systems.

---

[1] https://www.tristarrisk.com/#

[2] https://www.tristargroup.net/about-us

[3] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

Defendant launched an investigation with the assistance of third-party forensic specialists who determine that an unknown unauthorized party gained access to Defendant email environment beginning on November 4, 2022, and subsequent unauthorized access to certain systems containing consumer data. which contained Plaintiff's sensitive personal information (the "Data Breach"). Defendant's notice letter confirmed that Defendant investigated and determined that Plaintiff's personal information was contained in the database files accessed, exfiltrated, or acquired by unauthorized persons in the Data Breach. Defendant's notice letter also informed Plaintiff and other similarly situated Class members that the database files impacted by the Data Breach included their PII, including name, date of birth, and Social Security Number.

3. Defendant's data breach notice letter lacked details or information necessary for Plaintiff and Class members to understand the scope and severity of the Data Breach. Further, due to the nearly fifteen (15) month lapse in time between the Data Breach and Defendant's notice to Plaintiff and other affected individuals, unauthorized third parties who accessed and procured their PII had already been able to acquire and sell Plaintiff's and the Class members' PII on the black market or dark web, or otherwise fraudulently misuse their PII for nefarious purposes or personal gain. Although the exact number of affected customers is presently unknown, based upon information and belief at least 35,120 customers have been affected by the Data Breach nationwide.

4. Defendant owed Plaintiff and Class members a duty to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected and maintained for business purposes and stored on its servers, databases, and/or networks.

5. Defendant breached their duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access and storing and retaining Plaintiff's and Class members'

personal information on inadequately protected servers, databases, and/or networks.

6. The Data Breach happened because by Defendant intentionally, willfully, recklessly, or negligently failing to implement adequate cybersecurity, which caused Plaintiff's and Class members' PII to be accessed and acquired by unauthorized persons. Plaintiff and Class members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their PII; and (v) the present, continued, and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

7. This action seeks to remedy these failings. Plaintiff brings this action on behalf of themself individually and on behalf of all other similarly situated persons affected by the Data Breach.

VENUE AND JURISDICTION

8. This Court has subject matter of this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendant.

9. This Court has personal jurisdiction over Defendant because Defendant regularly conduct business in California and maintain offices, a headquarters, and/or principal place of business in California.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a

substantial part of the events, acts, and omissions giving rise to Plaintiff's claims and damages occurred in, was directed to, and/or emanated from this District.

PARTIES

11. Plaintiff is a resident and citizen of San Mateo County, in the State of California.

12. Plaintiff is a consumer who provided their personal information and PII to Defendant. Plaintiff has had their personal information and PII collected, stored, and/or maintained by Defendant since prior to November 10, 2022.

13. Plaintiff received a data breach notice letter dated February 1, 2024, and addressed to them from Defendant entitled "Notice of Data Breach." The letter indicated that Plaintiff's PII, including their name, date of birth, and Social Security number, at minimum, was improperly accessed, and acquired by unauthorized third parties through the Data Breach.

14. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII was accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons in the Data Breach.

15. Defendant TRISTAR Insurance Group, Inc. is a California corporation with its principal place of business and/or headquarters located at 100 Oceangate, Suite 840 Long Beach, California 90802, within this judicial district. Defendant at all relevant times conducted business in the State of California.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

16. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[4] California has repeatedly

[4] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has

recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

17. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

18. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[6] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

19. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[7]

20. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more

---

quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[5] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[6] *See* Soma, *Corporate Privacy Trend, supra*.

[7] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

21. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

22. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

23. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[11]

24. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[8] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[9] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576 160764037920274.

[10] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[11] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

Theft of PII Has Grave and Lasting Consequences for Victims

25. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

26. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[12]

27. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[13] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

28. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[14]

29. Identity thieves use personal information for a variety of crimes,

---

[12] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[13] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[14] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

including credit card fraud, phone or utilities fraud, and bank/finance fraud.[15] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[16]

30. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

---

[15] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer, or taxpayer identification number." *Id*.

[16] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[17] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying- about-identity-theft.

31. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[18] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[19] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[20]

32. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

33. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[21]

34. It is within this context that Plaintiff and thousands of similar individuals must now live with the knowledge that their PII is forever in cyberspace, putting them at imminent and continuing risk of damages, and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

---

[18] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[19] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[20] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[21] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

Defendant's Collection of PII

35. Defendant acknowledges that it obtains, stores, and transmits a substantial amount of sensitive personal consumer data. Defendant's Privacy Notice represents that it collects the following categories of personal information:[22]

- Basic personal and demographic information, such as your name, date of birth, age, gender, and marital status.
- Contact information, such as your address, telephone number and email address.
- Unique identifiers, such as identification numbers issued by government bodies or agencies (e.g., your national identifier number or social security number, passport number, ID number, tax identification number, driver's license number).
- Employment information, such as your job title, employer, employment status, salary information, employment benefits, employment history and professional certifications.
- Financial information, such as your bank account numbers, credit card numbers, brokerage account numbers, transaction information, tax information, details of your income, property, assets, investments, pension and benefits, debts, and creditworthiness.
- Policy information, such as our policy number, policy start and end dates, premiums, individual terms, claims history and claims data, mid-term adjustments, reasons for cancellation, risk profile and details of policy coverage.
- Claim information, such as claimant's relationship to policyholder/insured, and the date and particulars of such claim, including causes of death, injury or disability and claim number.
- Commercial information, such as records of your personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Events or meeting information, such as details about your visits to our offices (including CCTV), your interest in and attendance at events or meetings, audio recordings, photographs or videos captured during meetings, events, or calls with you.
- Special category data and sensitive personal data, such as data relating to your health (including protected health information), genetic or biometric data, sex life, sexual orientation, gender

[22] Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tristargroup.net/pdf/CCPA%20Privacy%20Policy%20Statement.pdf

identity, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership.

- Criminal records information, such as criminal charges or convictions, including driving offences, or confirmation of clean criminal records.
- Professional disciplinary information.
- Personal information received from background checks and sanctions screenings.
- Marketing information, such as your consent to or opt out from receiving marketing communications from us and/or third parties, your marketing preferences, or your interactions with our marketing campaigns and surveys, including whether you open or click links in emails from us or complete our surveys.
- Sites and communication usage information, such as your username, your password, other information collected by visiting our Sites or collected through cookies and other tracking technologies, including your IP address, domain name, your browser version and operating system, traffic data, location data, browsing time, and social media information, such as interactions with our social media presence.

36. In Defendant's separate "California Privacy Notice (CCPA-CPRA)"[23], Defendant also provide the PI they collect and disclose may include:

- Personal Identifiers such as your name, any alias, your mailing address, telephone number, email address, gender, date of birth, Social Security number, Driver's License number, passport number, your signature, your digital signature, and other similar identifiers;
- Personal information, including employment information, medical and health information, medical exams, reports, tests, procedures, and prescriptions.
- Financial and banking information such as bank account number, credit/debit card number, income and tax information;
- Characteristics of protected class or groups under state or federal law, including birthday, sex, marital status and the like;
- Commercial information, including the purchase of any medical or non-medical equipment relating to your claim;
- Internet or other electronic network activity information, including, but not limited to, IP address, browsing and search

[23] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.tristargroup.net/pdf/CPRA%20Privacy%20Notice.pdf

history, and information regarding a consumer's interaction with TRISTAR;

- Geolocation data such as physical location or movements;
- Audio, electronic, visual, thermal, or similar information such as voice messages, recorded statements and video evidence;
- Professional or employment-related information;
- Education information;
- Policy information, such as our policy number, policy start and end dates, premiums, individual terms, claims history and claims data, mid-term adjustments, reasons for cancellation, risk profile and details of policy coverage;
- Claim information, such as claimant's relationship to policyholder/insured, and the date and particulars of such claim, including causes of death, injury or disability and claim number;
- Events or meeting information, such as details about your visits to our offices (including CCTV), your interest in and attendance at events or meetings, audio recordings, photographs or videos captured during meetings, events, or calls with you;
- Marketing information, such as your consent to or opt-out from receiving marketing communications from us and/or third parties, your marketing preferences, or your interactions with our marketing campaigns and surveys, including whether you open or click links in emails from us or complete our surveys.
- Websites and communication usage information, such as your username, your password, other information collected by visiting our Websites or collected through cookies and other tracking technologies, including your IP address, domain name, your browser version and operating system, traffic data, location data, browsing time, and social media information, such as interactions with our social media presence.
- Special category data and sensitive personal data, such as data relating to your health (including protected health information), genetic or biometric data, sexual orientation, gender identity, racial or ethnic origin;
- Criminal records information, such as criminal charges or convictions, including driving offenses, or confirmation of clean criminal records;
- Professional disciplinary information; and
- Inferences drawn from any of the information identified above.

37. Defendant collects personal information from customers directly as well as through third parties such as insurers, consumer reporting agencies, Defendant's affiliated companies, or other third parties in the course of conducting Defendant's business.

38. For California customers, Defendant's Privacy Policy identifies the rights of California residents regarding their personal information pursuant to the California Consumer Privacy Act ("CCPA"). These rights include requesting disclosure of the information collected, the purpose for collecting the information, and any third parties with whom the information is sold or disclosed. Additionally, the rights under the CCPA identified by Defendant's Privacy Policy include requesting deletion of the personal information, opting out of have personal information sold to third parties, and receiving information that identifies any third party that has received personal information.

Defendant's Promise to Safeguard PII

39. Defendant represents that they understand the importance of protecting Plaintiff's and the Class members' personal information. For example, in its Privacy Notice, Defendant claim it implements, "a range of organizational and technical security measures to protect your personal data, including:

- Restricted access to those who need to know for the purposes set out in our underlying agreement or this Privacy Notice.
- Firewalls to block unauthorized traffic to servers.
- Physical servers located insecure location and accessible only by authorized personnel.
- Internal procedures governing the storage, access and disclosure of your personal data.
- Additional safeguards as may be required by applicable laws in the jurisdiction where we process your personal data."[24]

[24] Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tristargroup.net/pdf/CCPA%20Privacy%20Policy%20Statement.pdf

40. Defendant also promises that in sharing personal data with third parties, they require, "those third parties (where applicable) to maintain a comparable level of protection of personal data as set out in this Privacy Notice by the use of contractual requirements and other means."[25]

41. Defendant further promises that if personal data must be transferred outside the USA to certain third parties, "transfers of personal data will be subject to appropriate safeguards to ensure an adequate level of protection and compliance with applicable law."[26]

42. Defendant's Terms of Use Agreement expressly references Defendant's Privacy Policy and states the terms and conditions of the Privacy Policy are incorporated into Defendant's Terms of Use.

The Data Breach

43. On or about February 1, 2024, data breach notice letters were issued by or on behalf of Defendant announcing that on or about November 10, 2022, Defendant became aware of suspicious activity on certain computer systems. Defendant launched an investigation with the assistance of third-party forensic specialists who determine that an unknown unauthorized party gained access to Defendant email environment beginning on November 4, 2022, and subsequent unauthorized access to certain systems containing consumer data. which contained Plaintiff's sensitive personal information (the "Data Breach"). Defendant's notice letter confirmed that Defendant investigated and determined that Plaintiff's personal information was contained in the database files accessed, exfiltrated, or acquired by unauthorized persons in the Data Breach. Defendant's notice letter also informed Plaintiff and other similarly situated Class members that the database files impacted by the Data Breach included their PII, including name, date of birth, and Social Security Number.

---

[25] *Id.*
[26] *Id.*

44. Defendant's data breach notice letter provided little other information regarding the Data Breach itself. For instance, Defendant provided no information regarding how exactly the Data Breach occurred, how they identified Plaintiff and other affected individuals to send them notice, or how many people were affected by the Data Breach.

45. Defendant's data breach notice letter is spare on details, explaining only that:

> **What Happened?** On or about November 10, 2022, TRISTAR became aware of suspicious activity on certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to our email environment beginning on November 4, 2022, and that the unauthorized actor was ultimately able to gain access to certain TRISTAR systems beginning on November 9, 2022. Through our investigation, we learned that certain information related to our customers was potentially exfiltrated from TRISTAR's network. TRISTAR therefore undertook a comprehensive and time intensive review of potentially impacted files, with the assistance of third-party subject matter specialists, and later determined that the files contained certain information related to you. TRISTAR has seen no evidence of misuse of any information related to this event. Additionally, there is no evidence that TRISTAR or PROVIDENCE GROUP's claims or accounting systems were breached during this incident.
>
> **What Information Was Involved?** TRISTAR determined that the following information related to you was present within the impacted files: your name, BIRTH_DATE and SSN.
>
> **What We Are Doing.** Upon discovery, we immediately secured the environment and commenced an investigation to confirm the nature and scope of the event. We reported this event to law enforcement and are cooperating and assisting in their investigation. We also implemented additional technical safeguards, and reviewed policies and procedures relating to data privacy and security.

46. Defendant reported the Data Breach to the Office of the Maine Attorney General indicating that the Data Breach affected a total of 35,120 persons.[27]

[27] *Id.*

47. As a result of the Data Breach, Plaintiff has suffered an invasion and loss of their privacy, Plaintiff has noticed unauthorized use of their PII which Plaintiff attributes to the Data Breach. Plaintiff has spent time attempting to mitigate the damages caused by the Data Breach, including monitoring Plaintiff's personal financial accounts and consumer reports, disputing unauthorized activities and transaction, which is time that Plaintiff otherwise would have spent performing other activities or leisurely events for the enjoyment of life rather than feeling stressed, frustrated, and using their personal time trying to mitigate the impact of the Data Breach.

48. As a result of the Data Breach, Plaintiff is, and will continue to be, at heightened risk for financial fraud, and/or other forms of identity theft, and the associated damages resulting from the Data Breach, for years to come.

Defendant's Notice of Data Breach

49. Defendant's vague description of the Data Breach leaves Plaintiff and Class members at continuing risk. By failing to adequately inform Plaintiff and Class members of all the details surrounding the breach Plaintiff and Class members are unable to adequately protect themselves against identity theft and other damages. Further, Defendant offers Plaintiff and Class members little to assist them with any fall-out from the Data Breach or to advise them of the extent of the potential threat they face because of their sensitive PII where Plaintiff and Class members are now at increased risk of identity theft for years to come and the indefinite future as a result of the Data Breach.

50. Defendant also fails to explain why it took over fifteen (15) months from learning of the ransomware incident in November of 2022 to notify Plaintiff and Class members about the Data Breach on or about November 10, 2022. This delayed Plaintiff's and Class members' ability to be fully informed and take necessary precautions to protect themselves from identity theft and other fraud.

Defendant Knew or Should Have Known PII Are High Risk Targets

51. Defendant knew or should have known that PII like that at issue here, is a high-risk target for identity thieves.

52. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[28]

53. Prior to the Data Breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services have the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[29]

54. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable information (PII), they represent an attractive target for cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and

---

[28] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[29] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[30]

55. As such, Defendant were aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

Defendant Violated the Federal Trade Commission Act

56. Federal and State governments have likewise established security standards and issued recommendations to prevent and limit the impact of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

58. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[33]

59. The FTC recommends that businesses:

---

[30] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

[31] Federal Trade Commission, *Start With Security: A Guide for Business*, available at: https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Nov. 18, 2023).

[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Nov. 18, 2023).

[33] FTC, *Start With Security*, *supra* note 12.

- Identify all connections to the computers where you store sensitive information.
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
- Do not store sensitive consumer data on any computer with an Internet connection unless it is essential for conducting their business.
- Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.
- Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the Internet.
- Determine whether a border firewall should be installed where the business's network connects to the Internet. A border firewall separates the network from the Internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.
- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

60. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the

Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

61. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Defendant was at all times fully aware of its obligation to protect the personal and financial data of Plaintiff and Class members. Defendant was also aware of the significant repercussions when it failed to do so.

63. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class members' PII—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

64. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Plaintiff and Class Members Face a Substantial Risk of Imminent Harm

65. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[34] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[35]

66. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

[34] 17 C.F.R. § 248.201 (2013).
[35] *Id.*

67. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials and financial account information, or trick victims into paying them their money or disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

68. The Social Security Administration explains that:

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[36]

69. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[37]

---

[36] Social Security Administration, *Identity Theft and your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 19, 2023).

[37] United States Government Accountability Office, Report to Congressional Requesters, *Personal Information, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* June 2007, p. 29, https://www.gao.gov/assets/gao-07-737.pdf (last visited August 14, 2023).

70. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[38] Victims of the Data Breach, like Plaintiff and Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[39]

71. According to the Attorney General of California, "Getting a new social security number is probably not a good idea."

Victims of identity theft sometimes want to change their Social Security number. The Social Security Administration very rarely allows this. In fact, there are drawbacks to changing your number. It could result in losing your credit history, your academic records, and your professional degrees. The absence of any credit history under the new SSN would make it difficult for you to get credit, rent an apartment, or open a bank account.[40]

72. As a direct and proximate result of the Data Breach, Plaintiff and Class members have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and Class members must now expend considerable time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health

---

[38] Identity Theft Resource Center, *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces* (2021), available at: https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Nov. 19, 2023).

[39] *See* Federal Trade Commission, *Guide for Assisting Identity Theft Victims*, (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited Nov. 19, 2023).

[40] State of California Department of Justice, *Your Social Security Number: Controlling the Key to Identity Theft*, *available at:* https://oag.ca.gov/idtheft/facts/your-ssn (last visited Nov. 19, 2023).

insurance account information for unauthorized activity for years to come.

73. Plaintiff and Class members have suffered, and will continue to suffer, actual harms for which they are entitled to compensation, including for:

- Trespass, damage to, and theft of their personal property including PII;
- Improper disclosure of their PII;
- The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;
- The imminent and certainly impending risk of having their PII used against them by spammers and phishers to defraud them;
- Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;
- Loss of privacy suffered as a result of the Data Breach;
- Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;
- Ascertainable losses in the form of deprivation of the value of their PII for which there is a well-established and quantifiable national and international market;
- The loss of use of and access to their credit, accounts, and/or funds;
- Damage to their credit due to fraudulent use of their PII; and
- Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

74. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. To the extent that Defendant's legitimate business interests no longer warrant retaining their PII, copies of the PII should be destroyed.

75. The injuries to Plaintiff and Class members were, and will continue to be, directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

CLASS ACTION ALLEGATIONS

76. Pursuant to Federal Rule of Civil Procedure 23, Cal. Code Civ. Proc. § 382, and Cal. Civ. Code § 1781, Plaintiff seeks to represent and intends to seek certification on behalf of a "Nationwide Class" and a "California Subclass" (together referred to herein as the "Class") defined as:

> ***Nationwide Class***
> All persons within the United States whose personally identifiable information ("PII") was subjected to the Data Breach in November 2022, including all persons who received Defendant's notice of the Data Breach.
>
> ***California Subclass***
> All persons residing within the State of California whose personally identifiable information ("PII") was subjected to the Data Breach in November 2022, , including all persons who received Defendant's notice of the Data Breach.

77. Excluded from the Class are: (1) Defendant and their respective officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

78. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

79. Plaintiff reserves the right to modify or amend the definition of the proposed classes as appropriate.

80. Under Fed R. Civ. P. 23(a)(1), the Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, based on information and belief, the Class consists of tens of thousands of individuals, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is so numerous that joinder of all members is impractical.

81. Under Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

82. As brought under Fed. R. Civ. P. 23(a)(2) and (b)(3), there is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiff and Class members;

(b) Whether the Defendant's security systems and procedures complied with the applicable federal and state laws and regulations;

(c) Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class members;

(d) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(e) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members;

(f) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been stolen;

(g) Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII had been compromised;

(h) Whether an implied contract existed between Defendant on the one

hand, and Plaintiff and Class members on the other, and the terms of that implied contract;

(i) Whether Defendant breached the implied contract;

(j) Whether Defendant breached their duty to protect the PII of Plaintiff and each Class member; and

(k) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

83. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff have no interests adverse to or that conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection and consumer privacy class actions of this nature.

84. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

85. Defendant have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*
(On Behalf of the Plaintiff and the California Subclass)

86. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

87. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[41]

88. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

89. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the

[41] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

90. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

91. Plaintiff and the Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

92. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in and is headquartered in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households,

or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

93. The PII accessed and taken by unauthorized persons in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and other Class members' unencrypted names, mailing addresses, social security numbers and/or tax identification numbers, among other personal information.

94. Plaintiff's PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name, mailing address, social security number and/or tax identification number, at minimum, was wrongfully accessed, viewed, and/or taken by unauthorized persons in the Data Breach.

95. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

96. On or about April 10, 2024, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant do not, or are unable to, cure the violation within 30 days, Plaintiff will amend their complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

97. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff, individually and on behalf of the Class, seeks actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of the Plaintiff and the California Subclass)

98. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

99. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

100. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

101. Defendant also violated the UCL by failing to promptly notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to better safeguard and protect their PII and identities.

102. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

103. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

104. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

105. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Therefore, Plaintiff individually and on behalf of the Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate cybersecurity, data security practices, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION

Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.* (On Behalf of Plaintiff and the California Subclass)

106. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

107. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

108. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

109. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section

1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

110. Plaintiff and members of the California Subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

111. The PII of Plaintiff and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collect and which was impacted by the Data Breach includes an individual's name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) social security number; (ii) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

112. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the

California Subclass from unauthorized access, destruction, use, modification, or disclosure.

113. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California Subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

114. As a direct and proximate result of Defendant' acts or omissions, Plaintiff and the California Subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the California Subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

115. As a direct consequence of the actions as identified above, Plaintiff and the California Subclass members incurred losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the Data Breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal information disseminated that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

FOURTH CAUSE OF ACTION

Negligence
(On Behalf of Plaintiff and the Class)

116. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

117. Defendant owed various duties to Plaintiff and the Class, including pursuant to the CCPA, as alleged in detail above. In addition to other duties, Defendant owed a duty to Plaintiff and other Class members in safeguarding the personal information entrusted to it by Plaintiff and the Class members. Defendant both owed duties to Plaintiff and the Class with regard to their manner of collection, transmission, sharing, and maintenance of Plaintiff's and the Class members' personal data, including PII, and were required to maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class members personal information.

118. Defendant breached their respective duties by engaging in the conduct and omissions alleged above and in violation of the CCPA, UCL, and CRA, as well as each of their privacy policies as alleged above.

119. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and Class members entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant, based on Defendant's assurances that the information would be protected by superior data security practices.

120. Defendant was in an exclusive position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

121. Defendant has admitted that Plaintiff's and Class members' PII was wrongfully lost and disclosed to unauthorized third persons as a result of the Data

Breach.

122. Defendant was both the actual and legal cause of Plaintiff's and the Class members' damages.

123. Plaintiff believes and thereon alleges that as a proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer actual damages, invasion and loss of privacy, emotional distress, and other economic and non-economic losses as described herein and above.

124. Due to the egregious violations alleged herein, Plaintiff asserts that Defendant breached their respective duties in an oppressive, malicious, despicable, gross, and wantonly negligent manner. Defendant's conscious disregard for Plaintiff's privacy rights entitles Plaintiff and the Class to recover punitive damages.

FIFTH CAUSE OF ACTION

Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

125. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

126. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

127. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

128. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

129. Plaintiff and Class members are consumers within the class of persons

Section 5 of the FTC Act was intended to protect.

130. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

131. Additionally, Defendant has a duty to act reasonably in handling consumer data and to use reasonable data security measures arising under the Gramm-Leach-Bliley Act's implementing regulations, 16 C.F.R. § 314 (the "Safeguards Rule"), which "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information" and "applies to the handling of customer information by all financial institutions[.]" 16 C.F.R. § 314.1(a)-(b).

132. The Safeguards Rule "applies to all customer information in [a financial institution's] possession, regardless of whether such information pertains to individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [the subject financial institution]." 16 C.F.R. § 314.1(b).

133. The Safeguards Rule requires financial institutions and entities who act on behalf of financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the financial institution's] size and complexity, the nature and scope of [the financial institution's] activities, and the sensitivity of any customer information at issue." 16 C.F.R. § 314.3(a).

134. Specifically, the Safeguards Rule requires entities to:

> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer

> information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
> * * *
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

135. As alleged herein, Defendant breached its duties under the Safeguards Rule.

136. Defendant also has a duty under the California Constitution which contains a Right to Privacy clause, Article 1, Section 1, which states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending . . . privacy."[42]

137. Defendant's failure to implement reasonable measures to secure consumers' PII violates the California Constitution and the FTC Act.

138. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

---

[42] Calif. Const. Art. 1, § 1.

SIXTH CAUSE OF ACTION

Invasion of Privacy
(On Behalf of Plaintiff and the Class)

139. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

140. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

142. Defendant intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiff and Class Members.

143. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

144. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

145. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their relationships with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

146. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

147. Defendant acted with intention and a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

148. Because Defendant acted with this knowing state of mind, it had notice and knew its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class members.

149. As a proximate result of the above acts and omissions of Defendant, PII of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

150. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class members.

SEVENTH CAUSE OF ACTION

Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

151. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

152. Defendant required Plaintiff and Class members to provide their PII for them to obtain Defendant's services.

153. Defendant's Privacy Policy, advertising and marketing materials, and website representations made enforceable promises that Plaintiff's and Class members' PII would be kept secure and confidential, would be used only for legitimate purposes to serve Plaintiff and Class members, and would not be disclosed to unauthorized third parties.

154. Defendant promised to employ "a range of organizational and technical

security measures to protect your personal data, including:

- Restricted access to those who need to know for the purposes set out in our underlying agreement or this Privacy Notice.
- Firewalls to block unauthorized traffic to servers.
- Physical servers located insecure location and accessible only by authorized personnel.
- Internal procedures governing the storage, access and disclosure of your personal data.
- Additional safeguards as may be required by applicable laws in the jurisdiction where we process your personal data."[43]

155. Defendant promised to retain Plaintiff's and Class members' information only for as long as their account is active, for as long as needed to provide services requested, or as long as needed to comply with legal obligations.

156. Plaintiff and Class Members only provided their PII because there was an implicit agreement that Defendant would secure and protect their PII from disclosure to any unauthorized third party, and to timely and accurately notify Plaintiff and Class members in the event of a Data Breach.

157. Plaintiff and Class members would not have provided their PII to Defendant had they known that Defendant would fail to perform its promises to safeguard and protect their PII and provide accurate and timely notice of the Data Breach.

158. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

159. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach. More specifically, Defendant breached the implied contracts it made with Plaintiff and Class members by (i) failing to use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of Plaintiff's and Class members' PII, (ii) failing to encrypt

[43] https://tristargroup.net/pdf/CCPA%20Privacy%20Policy%20Statement.pdf

the PII in storage, (iii) failing to delete PII it no longer had a reasonable need to maintain, and (iv) otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

160. Defendant was both the actual and legal cause of Plaintiff's and the Class members' damages.

161. Plaintiff believes and thereon alleges that as a proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer actual damages, invasion and loss of privacy, emotional distress, and other economic and non-economic losses as described herein and above.

162. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class members are entitled to recover actual, consequential, and nominal damages.

EIGHTH CAUSE OF ACTION

Breach of Contract
(On Behalf of Plaintiff and the Class)

163. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

164. Plaintiff and Class members entered into express and/or implied contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from unauthorized disclosure.

165. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant in connection with its products and/or services.

166. Defendant breached their contractual obligation to protect the nonpublic personal information Defendant gathered when Plaintiff's and the Class members' personal information was accessed and acquired by unauthorized third parties as part

of the Data Breach.

167. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated a representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, individually and on behalf of the Class, further requests that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: April 10, 2024

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: */s/ Abbas Kazerounian*
Abbas Kazerounian, Esq.
Mona Amini, Esq.

Attorneys for Plaintiff